UNIVERSITI TEKNOLOGI MARA

GENERATING A RICH MOBILE DATASET USING A CENTRAL MANAGEMENT APPROACH

KHELWA FARIZA BINTI MOHD SAKRONI

Dissertation submitted in partial fulfillment
of the requirements for the degree of
Master of Science

Faculty of Electrical Engineering

July 2014

ABSTRACT

This project will brief reader with a comprehensive study on mobile Botnets. Bots are small-size malwares that infect computers or mobile network, which can join with other bots via the Internet to form a network of bots called Botnet. Botnets and their bots have a dynamic and flexible nature. The Botmasters, who control the Botnets, update the bots and change their codes day by day to avoid the traditional detection methods such as signature-based anti-viruses. Mobile environment is less protected and Botmasters have taken advantage of the lack of security knowledge of mobile users in an attempt to steal private data and earn money illegally. In addition, many techniques are employed by Botmasters to make their Botnets undetectable for as long as possible.

This primary purpose of this project is to presents a method to generate and produce rich mobile datasets for mobile security researchers. The approaches used to achieve this project are through literature studies of mobile Botnets, Botnets detections and mobile data collection software which run on the background of the mobile phones. Project development is carried out using Google Application, named tPacketCapture which been installed in the Android Smartphone and the collected mobile data been analyzed using a network protocol software, named Wireshark. The project result are expected that the propose method runs in the mobile Smartphone is able to be generate and capture the valid mobile dataset and these dataset able to analyze and evaluate as a rich dataset for future mobile security study.

ACKNOWLEDGEMENTS

Bissmillahirrahmanirrahim,

Alhamdulillah. Thanks to Allah S.W.T, The Most Gracious and The Most Merciful, whom with His willing give me the opportunity to complete this Final Year Master Project which is title '*Generating a Rich Mobile Dataset Using a Central Management Approach*'. This thesis was prepared to fulfill the requirement for the Master of Science (MSc.) in Telecommunication and Information Engineering for Faculty of Electrical Engineering, Universiti Teknologi MARA (UiTM).

Firstly, I would like to express my sincere gratitude to my Supervisor, Assoc. Prof. Dr. Habibah Binti Hashim, a senior lecturer at Faculty of Electrical Engineering, UiTM, for her endless ideas, motivation and guidance throughout the period of completing this project. Besides, I also want to thanks her PhD student, Meisam Eslahi for his assistance, support and cooperation during project progress that had given valuable information and suggestions in the compilation and preparation of this final year Master project.

My deepest thanks and appreciation also goes to my beloved husband, Muhammad Akmal Bin Abu Bakar, my parents, Mohd Sakroni Bin Alias and , and the rest of family for their understanding and tireless effort in building stream of myself. Their encouragement, constructive suggestion and full of support for the thesis completion, from the beginning till the end. Also thanks to all of my friends and classmates, those have been contributed by giving a moral supports for my work during the project progress till it is fully completed.

Last but not least, my thanks to all the lecturers and staffs of Faculty of Electrical Engineering UiTM, for the great cooperation during my Final Year Master Project.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW AND BACKGROUND OF THE PROJECT

Nowadays, mobile devices are everywhere and the Smartphone usage has dramatic growth in mobile network. It is beyond just simply making phone calls. Among the mobile's operating systems, Android is very popular owing to availability as an open source operating system. Due to the proliferation of Android malwares, it is crucial to study the best classifiers to detect them effectively and accurately. [35]

Internet is most vulnerable to attacks due to its public nature and virtually without centralized control. With the growing financial dealings and business dependence on Internet, these attacks have increased. Whereas previously hackers would satisfy themselves by breaking into someone's system, in today's world hackers' work under an organized crime plan to obtain illicit financial gains or profits. Various attacks or malicious activities like spamming, phishing, click fraud, distributed denial of services (DDoS), hosting illegal material, key logging, click fraud, adware or thieving personal information are being carried out by hackers using Botnets [36, 39, 41, 42, 44, 43].

Among all these threats, Botnet is considered the most dangerous and biggest threat to cyber security [39, 40]. Botnets will increasingly adopt the most advanced permutations of resilient lookup techniques into the future [37, 38]. A Botnet is a linked group of infected networks (termed as Bots). Bot is a computer program installed on a